基于Symbian S60平台的手机取证技术研究

周靖哲　吴晓涛

摘　要：手机中存储的与日常相关的信息是智能手机最宝贵的财富，是办案人员进行案件跟踪的重要线索来源，如何获取手机中的数据便成为了手机取证研究的重要课题。本文以Symbian S60手机平台为研究对象，介绍了Nokia智能手机三种常用的数据提取方法，并以获取手机中短信、通话记录、第三方应用数据为例，详细说明了数据提取的过程。

关键词：Symbian S60　数据提取　SDK　PC Suite

一、概述

Symbian智能操作系统由于其内存需求量小、功耗低，具有超长的手机待机时间，深受广大用户的喜爱，也使其广泛应用于智能手机中。智能手机作为人们日常生活中不可或缺的角色，除了具备手机通话的基本功能外，还具备了PDA的大部分功能，特别是对个人信息管理，手机上存储的用户日常信息才是智能手机最宝贵的财富。日常信息通常包括：短信息、通讯录、通话记录、电子邮件、QQ、MSN等。这些与日常相关的信息，在案件跟踪过程中，对于搜寻嫌疑人的线索具有重要的意义。本文以短信、通话记录以及第三方应用数据中QQ聊天记录的提取为例，详细介绍了基于Symbian S60平台的数据提取技术。

二、相关知识介绍

（一）Symbian S60的SDK

SDK，即软件开发工具包（Software Development kit），是辅助进行某类软件开发的工具、示例以及开发文档的集合。不同类的软件开发，所提供的SDK各有差异。Nokia的智能手机平台多采用Symbian S60平台，Symbian S60集成的SDK能够利用QT、C++、JAVA技术以及WEB技术进行应用的开发，这些SDK中包括了进行应用开发所必须的核心资源，包括API参考、应用开发示例代码、S60模拟器以及相关支持文档。

API，即应用程序接口（Application Programming Interface），是Symbian S60平台留给基于其应用程序开发的调用接口，应用程序通过调用系统SDK的API，可使操作系统执行应用程序的命令。因此，要获取Symbian S60平台的数据，可调用SDK提供的相关API，让手机操作系统执行相关API的操作方法，获取目标数据。

（二）PC Suite Connectivity API

Nokia的PC套件是使Nokia移动电话和计算机正常连接的应用软件的集合，提供手机数据的备份、同步、安装软件等功能。PC Suite Connectivity API是Nokia PC套件的集成部分，是Nokia PC连接SDK的扩展，免费为应用程序开发者提供手机与PC机的连接、手机协议的传输等，因此，可利用PC Suite Connectivity API，直接访问手机端部分数据，并进行提取。

三、数据提取方法

提取手机数据最直接的方法是调用PC Suite Connectivity API，但由于该API提供方法的局限性，只能提取部分手机数据，因此对于手机中不同的数据，其提取方法也各有差异。Nokia智能手机常用的三种数据提取方法如下：

（1）借助于Nokia公司提供的PC Suite Connectivity API3.2，调用相应接口，将手机中的短信，通讯录，日历，备忘录等信息提取出来。

（2）使用Symbian操作系统的SDK编程，利用系统自身API，将手机中的数据提取并存放到手机端，然后使用PC Suit API将这些数据提取到PC端，如通话记录。

（3）通过调用PC Suit API，将存储数据的文件提取到PC端，分析文件底层编码格式，将文件中的数据以字节为单位进行解码，如第三方应用QQ聊天记录的提取。

四、数据提取过程

本节分别以短信、通话记录、QQ聊天记录的提取为例，详细说明提取过程。

（一）短信的提取

调用PC Suite Connectivity API接口，获取短信手机数据。PC Suite Connectivity API类似于第三方库文件，可直接加载到工程文件中进行使用。要获取目标（短信）数据，其步骤如下：

（1）使用API中DAOpenCA方法打开短信内容，即获得目标句柄，如下：

DAOpenCA(IMEI, &dwMedia, CA_TARGET_SMS_MESSAGES, &hSMS);

（2）获取所提短信的路径：

CAGetFolderInfo(hContact, &pFolderInfo);

（3）由于数据量多，获取所要提取数据的ID：

CAGetIDList(hContact, 0, 0, &calDList);

（4）定义需要进行的操作，有读、写、删除操作，此处定义读操作：

CABeginOperation(hContact, 0, &hOperHandle);

（5）遍历读取目标数据：

CAReadItem(hOperHandle, &calDList.pUIDs[k], 0, CA_DATA_FORMAT_STRUCT, (LPVOID*)&dataContact);

（6）释放（1）步中打开的目标句柄：

CAFreeItemData(hContact, CA_DATA_FORMAT_STRUCT, (LPVOID)&dataContact)。

根据以上方法，不仅可以获取短信，也可获取通讯录，日历，备忘录信息。读取完数据后，直接将数据存放在PC端的文本文件中，便于后台展示调用。

（二）通话记录的提取

Symbian S60采用文件方式存储通话记录，即通话记录数据库。其在手机中的位置在C:\Private\101f401d\Logdbu.dat，以数据库文件格式存储。由于无法知道数据在数据库中的存储结构，造成无法直接对底层二进制文件进行解析还原，因此，只能借助于Symbian S60的SDK接口编程，编写一个运行于手机端的应用程序，提取所需的通话记录信息，并将数据存储在手机端。

SDK中通话记录客户端类CLogClient可操作通话记录数据库，它可以创建一个对本地通话记录数据库的会话。会话开启，当成功建立连接后，通过ClogViewEvent类访问数据库，并读取数据库中的信息，包括通讯时间、通讯号码、通讯日期、对方名称、持续时间等。

//提取通话记录数据函数，并将提取的数据，存入ClogEvent通话记录事件类

CLogClient::GetEvent(CLogEvent&aEvent, TRequeststatus&astatus)

//CLogClient创建会话成功后，通话记录事件操作类ClogViewEvent用户通过客户端会话读取通话记录具体事件

ClogViewEvent::Event（）

通话记录事件类CLogEvent，主要用于提取、存放、修改通话记录的具体数据，一个类实例对应一条通话记录，主要记录内容为描述信息、通讯方向、事件类型、对方称谓，号码。

数据提取的过程如下：

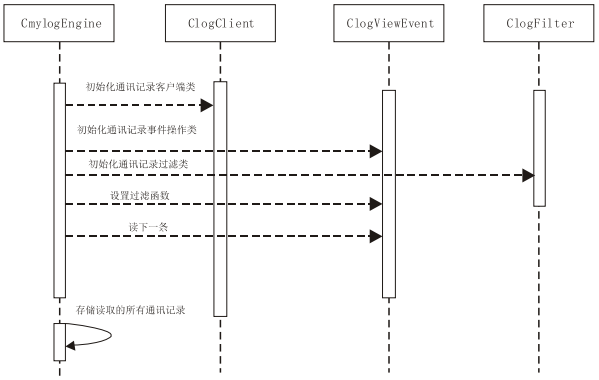

图1 通话记录操作实例

如图1所示，先初始化通话记录客户端类CLogClient、通话记录事件操作类ClogViewEvent，然后发出数据读取异步请求操作，完成数据的读取。将读取的多条通话记录，通过存储通讯事件，存入到数组中。设置过滤函数，遍历分析通话记录数组，将满足过滤条件的数据一条一条导出到文件，读取通话记录具体数据，存入各字符串变量，这样就可以将通话记录数据提取，然后将字符串变量中存储的一条一条的通话记录生成文本文档，存储于手机端。再利用PC suit API将提取的数据从手机端拷贝到PC端，便于与后台对接显示。其形式如图2所示。

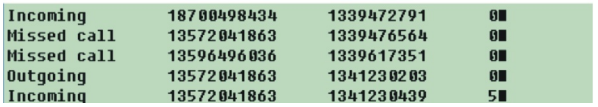

图2

（三）QQ聊天记录的提取

不同的QQ版本，其底层文件存储结构不同，本节以QQ2009的聊天记录的提取为例进行说明。Symbian S60平台QQ2009和QQ2010其聊天记录存储的文件结构相同，且在手机中存储的位置也一致。因此，对于

Symbian QQ2009和2010其数据提取方法一样。

在Symbian S60平台下，QQ聊天记录是以数据文件的形式存储。聊天记录文件的位置在C:\System\data\Tencent\QQ\自己的QQ号\对方的QQ号\msg.info。因此，首先要对手机文件的目录进行搜索以找到目标文件，并将其提取至PC上，然后进行解析。

具体步骤如下：

（1）使用PC suit API提取目标文件至PC，利用API中CONACopyFile函数将手机中的msg.info文件复制到PC端。函数原型为：

```
PCCS_FSAPI  CONACopyFile(FSHANDLEhFS Handle,
                         DWORD dwOptions,
                         const WCHAR* pstrFileName,
                         const WCHAR* pstrSourcePath,
                         const WCHAR* pstrTargetPath);
```

具体使用方法可以参考PC Suit API帮助文档和示例程序。

（2）打开并分析msg,info文件二进制数据结构，确定聊天记录在文件中存储的形式。QQ2009的msg.info文件的格式如表1所示。

表1 msg.info文件格式

部分	Begflag	Time	Fill	Direction	Msgbody	Endflag
长度(byte)	2	4	6	1	不定	2
说明	开始标志，A8 xx，xx表示Msgbody字节数	聊天时间	填充字节，无意义，6个0	表示消息是发出还是接收	消息体	结束标志，内容同Begflag

每条消息都以一段数据出现，一般格式为：

A8 XX SS SS SS SS 00 00 00 00 00 00 80 {MSG}A8 XX

如表1所示，每一条完整的消息，都是以“A8 XX”开头，XX表示消息体（MSG）的字节数，后面的四位SS SS SS SS表示时间，时间数据之后的是六位填充字节，用六个00表示，紧跟其后的一个字节表示消息的发送和接收（80为发送，00为接收），然后便是消息的内容数据，最后是结束标志A8，XX。

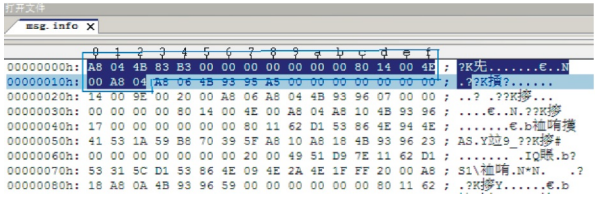

图3 msg.info文件示例

打开的msg.info格式的记录文件的十六进制编辑如图3所示。

确定聊天记录对应数据。某一条聊天记录对应的编码就是图中蓝色框区域，前面编码部分是其在底层存储的格式，后面，类似于乱码部分是其对应的数据。根据表1，4B 83 B3 00对应就是一条记录对应的时间，00 80表示该条记录是发出的消息，14 00 4E 00对应聊天内容。因此只要对这条记录进行相应解析，提取相应内容，进行存储，就可以将所有的聊天记录提取出来。

记录采用UTF-16编码格式，要对其进行解码还原，就要查找该种字符编码对应的汉字，按照字节进行解码还原即可。

在对时间进行解码时，要注意其是一个毫秒数，是相对于1970年1月1日0时0分0秒到现在的毫秒数。计算时高位在前，低位在后，直接把四个字节的16进制数转为10进制数即可。

五、总结

本文主要以Symbian S60的数据获取为研究对象，结合Symbian S60的Nokia提供的各种应用API特征，以短信、通话记录、QQ聊天记录为例，介绍了三种典型获取手机端数据的方法。当直接调用PC suite connectivity API无法获取数据时，可使用Symbian自身的SDK编程，这种方法可获取手机中大部分数据，但其操作要比直接调用PC suite connectivity API复杂的多；或是采用直接解析底层数据流文件格式的方法，对数据进行提取还原。虽然不同平台手机数据的获取存在一些差异，但Symbian平台数据的提取方法，对于其他平台数据的获取，具有一定的参考价值。

参考文献

[1]王佳,韩涛.基于Symbian的短信拦截技术的研究与实现[J].湖北大学学报,2011,3.

[2]郑少帅.基于Symbian OS的信息获取技术的研究[D].厦门大学,2009,6.

[3]祁创明.手机短信的证据属性及其提取方法[J].警察技术,2009,1.

[4]戴吉明.手机取证及其电子证据获取研究[J].计算机与现代化,2007,5.

[5]http://www. PC Suite – Nokia Developer Wiki.mht.